TEST PROJECT

BRICS-FS-27_IT Network Systems Administration

2022 BRICS Skills Competition

Module A network cabling and equipment configuration

Score: 100 points
Competition time: 120 minutes

Project introduction:

Hello, network engineers from the IT Department of Yang Wei International Information Co., Ltd.:

Headquartered in Beijing, our company has technology research and development, product manufacturing, marketing, finance, human resources, IT and other departments, and has an office in Wuhan.

In recent years, with the rapid development of China's digital economy, our business scope and business scale are also growing rapidly. In order to meet the company's high-quality development needs and create a good office environment for employees, we urgently need to explore new office locations and prepare to set up a branch in Shanghai.

From today on, we will start to build a network for the newly established branch and do a good job in network system management.

Task 1: network cabling scheme design

Task background:

Engineers, our newly established Shanghai Branch has confirmed the site selection, and the address is the seventh and eighth floors of Lianchuang SOHO. We should first carry out generic cabling design and cabling engineering implementation for the new office location, then install and configure network equipment such as switches, and finally carry out system testing.

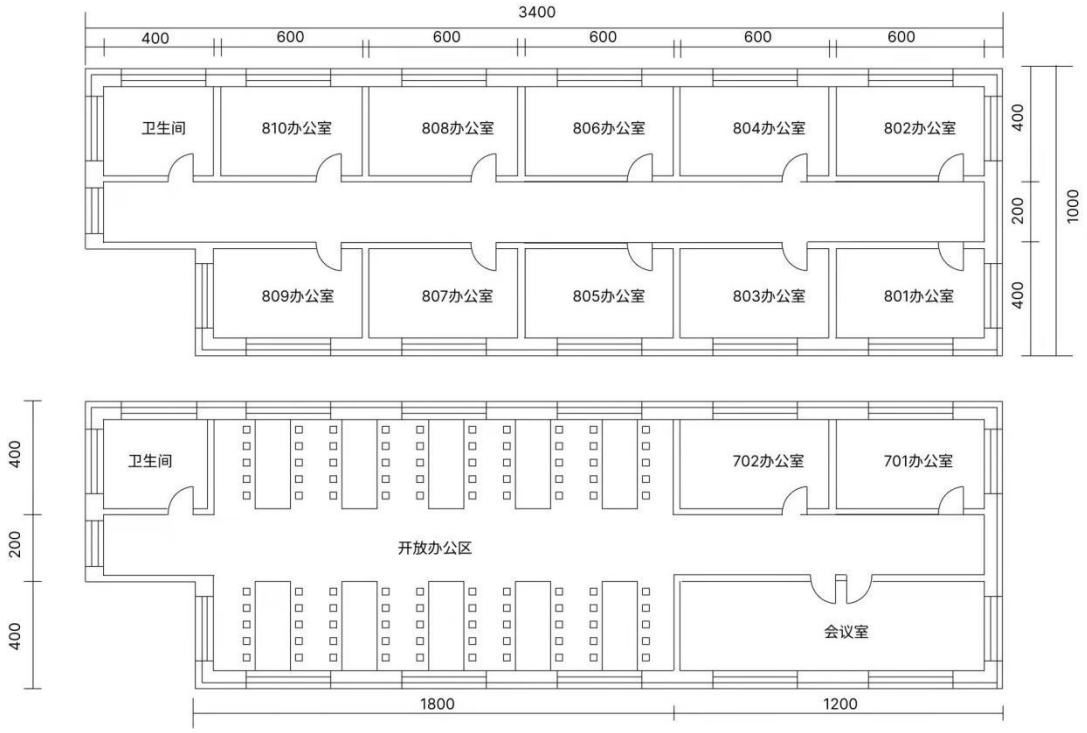
Please complete relevant specific tasks within the specified time according to the information and data provided below.

Task description:

According to the building plan and wiring requirements, the generic cabling design is carried out for the new office location.

Information:

1. Plane design drawing and function planning



Floor 7: about 34 meters long, 10 meters wide, and 4 meters high. There is an open working area (with 100 stations) about 18 meters long, a conference room (12 people) about 12 meters long, and two offices (4 people each) of 6 meters each, of which office 701 is the company's network computer room. See the schematic diagram of the 7th floor for details

Floor 8: the length and width are the same as those of the 7 floors. There are 10 offices, room 801-810 (4 people in each room), each of which is about 6 meters, and they are the administrative offices of the company. See the schematic diagram of 8th floor for details

2. Generic cabling requirements

（1）The branch adopts 1000m as the backbone network, 100m to the desktop, and super class 5 twisted pair;

（2）The branch adopts firewall structure for access, which is used to synchronize business data with the headquarters, and network interconnection equipment (firewall, router, switch and its equipment);

（3）According to the department setting of the branch company, it is divided into five vlans: product (vlan6), R & D (vlan5), training (vlan9), marketing (vlan8) and consulting (vlan2). The server group is one vlan (vlan7). Vlans cannot be visited each other. Only the product and R & D department can access the vlan of the server group and the server group communicates with the group through VPN;

（4）The branch has www server, financial server and company business application server, which are used for the company's daily business needs and network management;

（5）The branch company adopts the database based on MySQL as the development platform.

Requirement:

1. Based on the given building plan, the generic cabling design is carried out, and the drawing software is used. Considering the subsequent expansion and maintainability of the network system, the star topology is adopted:

（1）Each station is used as an information point, and the number of firewalls and routers is 1. CAD is used to draw the design scheme. Save it as PNG format picture, and upload it to the competition system;

（2）According to the design scheme of the previous task, the network consumables are estimated, including the length of super class 5 twisted pair, the number of computers, the number of switches (24 ports) and firewalls.

2. Use Visio drawing software to draw the branch network topology, save it as PNG format picture, and upload it to the competition system.

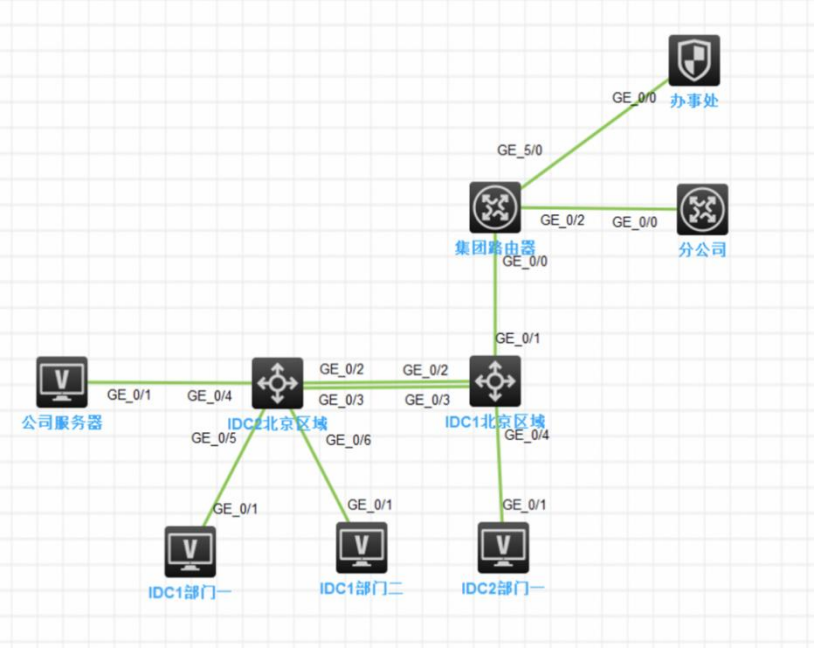
Task 2: network equipment configuration and testing

Task description:

Realize network interconnection and interworking among the group, Beijing data center, branches and offices.

Data and requirements:

1. Network topology:



IDC1 Beijing area and IDC2 Beijing area are the core exchanges of the company group. Group routers, branch routers and office firewalls are used for network interconnection.

(Please note: in this typical Internet application network architecture, as an IT network operation and maintenance personnel, please build a complete system environment according to the topology, so that the overall network architecture has good stability, security and scalability. Please test from the client after completing all service configurations to ensure that the corresponding applications can be accessed normally.)

2. Network connection table:

Equipment A connected to Equipment B			
Equipment name	Interface	Equipment name	Interface
IDC2 Beijing area（SW）	GE1/0/2	IDC1 Beijing area（sw）	GE1/0/2
IDC2 Beijing area（SW）	GE1/0/3	IDC1 Beijing area（sw）	GE1/0/3
IDC2 Beijing area（SW）	GE1/0/4	Company server（server）	GE1/0/2
IDC2 Beijing area（SW）	GE1/0/5	IDC1 Department I	GE1/0/1

IDC2 Beijing area（SW）	GE1/0/6	IDC1 Department I	GE1/0/1
IDC1 Beijing area（SW）	GE1/0/4	IDC1 Department I	GE1/0/1
IDC1 Beijing area（SW）	GE1/0/1	Group router	GE1/0/0
Group router	GE1/0/2	Branch router	GE1/0/0
Group router	GE1/0/5	Office	GE1/0/0

3. Network equipment allocation table

Equipment name	Equipment interface	IP address
IDC2 Beijing area	GE1/0/2	10.60.254.11/30
	GE1/0/3 Configure VLAN trunking	
	GE1/0/4 Server network segment（vlan30）	172.16.30.1~254/24
	GE1/0/5（vlan10 Marketing 1）	172.16.10.1~254/24
	GE1/0/6（vlan20 Product 1）	172.16.20.1~254/24
	GE1/0/7（vlan40 Legal affairs 1）	172.16.40.1~254/24
	GE1/0/8（vlan50 Finance 1）	172.16.50.1~254/24
	GE1/0/9（vlan60 HR 1）	172.16.60.1~254/24
IDC1 Beijing area	GE1/0/1	10.60.255.5/30
	GE1/0/2	10.60.254.12/30
	GE1/0/3 Configure VLAN trunking	
	GE1/0/5（vlan10 Marketing 1）	172.16.10.1~254/24

	GE1/0/6（vlan20 Product 1）	172.16.20.1~254/24
	GE1/0/7（vlan40 Legal affairs 1）	172.16.40.1~254/24
	GE1/0/8（vlan50 Finance 1）	172.16.50.1~254/24
	GE1/0/9（vlan60 HR 1）	172.16.60.1~254/24
Group routing	GE1/0/2	10.60.254.12/30
	GE1/0/5	10.60.253.6/30
	GE1/0/0	10.60.255.6/30
Group router	GE1/0/0	10.60.254.14/30
Office	GE1/0/0	10.60.253.7/30

4. Switch configuration

（1）In order to reduce broadcasting, VLANs need to be planned and configured according to the requirements of the topic. It is required that the configuration is reasonable. Unnecessary VLAN data flow is not allowed on all links, including VLAN1. At present, only VLAN10, VLAN20, VLAN30, VLAN40 and VLAN50 are allowed to pass through the bare optical fiber channel between the core switch IDC2 Beijing area and the core switch IDC1 Beijing area and the configuration of VLAN and interface description information is prohibited.

（2）Two bare optical cable channels are rented from the rental operator for the line between the core switch IDC2 and the core switch IDC1 has to realize the interworking between two DCS, one bare optical cable channel to realize the three-layer IP service bearing, and one bare optical cable channel to realize the two-layer service bearing. Specific requirements are as follows:

First, configure the maximum transmission unit of the bare optical cable channel carrying the three-layer IP service to be 1500bytes;

Second, at present, only one bare optical cable channel is designed to carry the layer-2 service. In order to cope with the growth of the layer-2 service traffic in the future, relevant technologies are configured to facilitate the subsequent link expansion and redundant backup. The number is 1;

Third, configure the core switch to share the load by using the source MAC address and

destination MAC address of the message;

Fourth, using CBQ to restrict the marketing business network segment of "IDC2 Beijing area", the bandwidth occupied by receiving and sending data is 3096kbp and 1024kbp respectively; "IDC1 Beijing area" limits the bandwidth occupied by receiving and sending data of the product network segment to 2048bps and 1024bps respectively;

Fifth, configure the MAC (0014-222c-aa69) of the server as a static MAC address table entry, so that the messages sent by the user to the server are only sent from GigabitEthernet1/0/4 unicast. Discard the message with MAC address 00a0-fc00-583c. Turn on the MAC information function of GigabitEthernet1/0/9 port, and the sending time interval is 300 seconds. Configure the device to send Syslog information to the log host (host address: 192.168.1.10);

Sixth: it is known that the NTP server is 109.120.2.191, and the server time is international standard time. Please configure this function on all switches to ensure that the clock of the switch is consistent with Beijing time.

5. Router configuration

It is planned to use OSPF agreement within the group and between the group and Guangdong Office. The process number used within the group is 1, and the process number used between the group and Chengdu office is 12. The specific requirements are as follows:

（1）The area between the core switches IDC1 and IDC2, the area between the group router and IDC2, and the area between the group router and the branch router are all backbone areas; The area between the group router and the office firewall is a common area, and the area number is 20;

（2）Adjust the time interval between all interfaces of OSPF process number 1 to send hello packets to 5 seconds. If the interface does not receive the other party's Hello message within 3 times of the time, it is considered that the opposite neighbor has failed;

（3）IDC1 and IDC2 are only allowed to publish business routes of marketing network segments; The office firewall releases its own marketing and product network segment business routes respectively. The business segment routes in the routing table of core switches IDC1 and IDC2 OSPF process 1 only allow you to learn the default routes of type 1 advertised by the office firewall and the group marketing business segment routes.

6. Firewall configuration:

（1）In 2022, the network protection action is about to be carried out, and the default rule of

adjusting the firewall security policy of the whole network is to refuse; On the firewall of the office, the product business network segment of the office can only access the https and MySQL database type businesses of the group product network segment, and the group marketing network segment can access any port of the marketing business network segment of the Guangdong Office;

（2）Configure network address translation in the firewall of the office. In the NAT address translation conditions, the source and destination IP are all any, and the public NAT address pool is 202.60.21.0/28; Ensure that all sessions generated by each source IP will be mapped to the same fixed IP address, generate log information when there is traffic matching this address translation rule, and send the matching log to UDP 514 port of 100.61.11.122; Turn on relevant features to expand the network address port resources after NAT conversion;

（3）The firewall of the office turns on the TCP SYN packet check function of the security gateway, and the connection is established only after checking that the received packet is a TCP SYN packet; Configure the maximum data segment that all TCP packets can transmit each time to be 1460, and try to reduce network fragmentation; Configure to check the establishment time of TCP three handshakes. If the three handshakes are not completed within 1 minute, the connection will be disconnected;

（4）The outlet bandwidth of the office is 800Mbps, which makes more rational use of outlet resources for the four business network segments of R & D, marketing, administration and finance within the group. When the export bandwidth is less than 480Mbps, the maximum upstream and downstream bandwidth of each IP is 5Mbps; When the outlet bandwidth is greater than 720Mbps, the maximum upstream and downstream bandwidth of each IP is 2Mbps, and the rule name is JT. At the same time, the bandwidth growth rate is required to be 2 times during the traffic change. At any time, it is necessary to ensure that the web access service accounts for 40% of the bandwidth per IP. FW-1 requires that the number of sessions per IP in the intranet is limited to 300.

Task 3: write Python script to realize network test automation

Task description:

Use Python script to search which IP addresses are idle and complete automatic operation and maintenance.

Requirements:

1. Write a code program that generates 192.168.1.1~192.168.1.254 according to the XOR method of Python;
2. Use Python's xxx package to randomly change the color of the IP generated by the first question. Red represents occupied, green represents idle. And convert the IP into *, and output a 16*16 matrix;
3. The group network has multiple networks, and the multi process method is used to calculate the number of idle IPS of 192.168.1.0/24, 192.168.2.0/24 and 192.168.3.0/24 at the same time.

Module B cloud network construction and operation and maintenance

Score: 100 points

Competition time: 180 minutes

Project background:

Engineers, the branch company has completed the network wiring and equipment configuration. In view of the complex business volume of the branch, it has high requirements for the carrying capacity and operation and maintenance services of the company's data center. In order to save hardware costs, allocate resources on demand and recover them quickly, a private cloud platform is built in the branch.

Please complete specific tasks within the specified time according to the information and data provided below.

Task 1 basic operation and maintenance tasks

Task description

Configure the basic environment of OpenStack server.

Requirements:

1. Add a new test user for the server at the node;
2. Update the image source on the node;
3. Configure the hostname on the node;
4. Configure the mapping relationship between the IP and hostname of the hosts file on the node.

Task 2 OpenStack setup task

Task description:

Deploy OpenStack cloud platform virtualization environment.

Requirements:

1. OpenStack platform basic services (rabbitmq, mariadb, memcache, Apache);
2. Configure OpenStack keystone components;
3. Configure OpenStack Glance components;
4. Configure OpenStack Nova components;
5. Configure OpenStack Neutron components;
6. Configure OpenStack dashboard components.

Task 3 OpenStack cloud platform operation and maintenance

Task description:

Configure IP address segment, subnet, security group and other sub services in the private network through OpenStack.

Requirements:

1. Use openstack command to create intranet (network name is inner), intranet subnet (network name is inner-sub), and set intranet subnet segment 10.0.0.0/24;
2. Use the openstack command to create an external network (Network Name: exter) and an external subnet (Network Name: exter-sub), and set the external subnet segment 192.168.5.0/24;
3. Use the openstack command to add a route (named router) and an intranet interface;
4. Use the openstack command to create the test security group, configure the rules, and open all ICMP, all TCP, and all TCP entry direction rules;
5. Use openstack related commands to create users. The naming format is, for example (Name: Li Si, user name is ls, which is composed of initials and lowercase abbreviations) password: passwd; Create project test; Bind the user role.

Task 4 OpenStack cloud platform operation and maintenance development

Task description:

Install the system in batches through scripts (take the cirros mirror image as an example, which is under the path /opt/ by default).

Requirements:

1. Create hosts in batches with scripts;
2. Shut down and start the host in batches with scripts;
3. Disable the host security port in batches with scripts.

Module C operating system network service configuration

Score: 100 points
Competition time: 120 minutes

Project background

Engineers, based on the completion of the comprehensive wiring of office networks and the establishment of private cloud platforms throughout the company, in order to improve the overall efficiency of the company's information network and strengthen the IT system operation and maintenance management service capacity. The whole network operation and maintenance structure needs to be designed, and the network management of the company headquarters, Wuhan Office and Shanghai Branch has entered the daily operation and maintenance.

Please complete specific tasks within the specified time according to the information and data provided below.

Task 1: system configuration and optimization

Task description:

Carry out network configuration and system optimization for Linux system to prepare for the deployment of applications and middleware.

Requirements:

1. Modify the /etc/sysconfig/network-scripts/ifcfg-ens192 network card configuration file. The configuration information is: gateway 10.5.5.2, IP static address 10.5.5.10, ONBOOT set to yes, NETMASK 255.255.255.0, DNS2 address set to 8.8.8.8. (Note: the network card does not need to be started in the docker container).
2. System kernel optimization: Please complete the following 13 kernel optimization parameters and write them to /etc/sysctl.conf file (configuration only, no need to take effect)

（1）NAT enables IP forwarding support;

（2）Open SYN Cookies. (Note: when SYN waiting queue overflow occurs, enable cookies to handle it, which can prevent a small number of SYN attacks. The default is 0, which means closed, 1 means open);

（3）Please enable TIME-WAIT sockets to be used for new TCP connections again (the default is 0, which means closed, and 1 means open);

（4）Turn on the rapid recycling of TIME-WAIT sockets in TCP connection (the default is 0, which means closed, and 1 means open);

（5）The world of the FIN-WAIT-2 state is set to 30s (indicating that if the socket is required to be closed by the local end, this parameter determines the time it remains in the FIN-WAIT-2 state. 60s by default)；

（6）The frequency of TCP sending keepalive messages is set to 20 minutes (indicating the frequency of TCP sending keepalive messages when keepalive is enabled. 2 hours by default);

（7）The port range of external connection is changed to 1024 to 65000. (It indicates the port range used for outward connection. It is small by default: 32768 to 61000);

（8）The length of the SYN queue is set to 8192. (It indicates the length of SYN queue, which is 1024 by default. Increasing the length can accommodate more network connections waiting for connection.);

（9）The maximum number of sockets of TIME_WAIT maintained by the system at the same time is 5000. (It indicates the maximum number of TIME_WAIT sockets the system maintains at the same time. If this number is exceeded, the TIME_WAIT sockets will be cleared immediately and a warning message will be printed. 180000 by default);

（10）Close ipv6;

（11）It indicates that when the rate of receiving packets by each network interface is faster than the rate of processing these packets by the kernel, the maximum number of packets allowed to be sent to the queue is modified to 262144;

（12）Please set the number of SYNACK packets sent by the kernel before giving up the establishment of the connection to 1;

（13）Please set the number of SYN packets sent by the kernel before giving up the establishment of the connection to 2.

3. Modify /etc/security/limits.conf file. Set the root user handle limit to 30000.

Task 2: project implementation

Task description:

In the optimized Linux server, install and deploy applications and middleware to avoid network vulnerability intrusion. It requires the security configuration and parameter optimization of MySQL, Nginx and Redis installed, database backup and expired data cleaning.

Requirements:

Note: the path of the system application deployment program installation package /data/package

1. Create the /data/service/ directory, install the jdk, the installation directory is /data/service/jdk, and configure the system environment variables;
2. Deploy MySQL: Deploy MySQL on the server, and install MySQL in binary installation mode. The installation directory is /usr/local/mysql, and the database directory is: /usr/local/mysql/data. Log in and change the root password to: qwe123456, create an account: jz, jz account password: qwe123456, create an application database mock_db, initialize data, authorize the JZ account to read and write the database mock_db, import data file mock_db.sql, create a scheduled task, backup the whole database at 1 a.m. every day, create a database cleaning script, and add the scheduled task data backup file for 20 days;
3. Deploy Redis: deploy Redis on the server. Install redis by compiling and installing. The installation directory is /data/service/redis. Modify the configuration file: add password authentication login. Password: qweiodks569PK. Start and check whether it is normal;
4. Java application deployment: start the Java application and port under /data/service/ according to the provided Java application file;
5. Nginx server setup: Deploy Nginx by yum, start, create a virtual machine, configure the static resource directory as /data/service/nginx/html, and put the static resources in /data/package/dist/ directory into it.

Task 3: automatic early warning

Task description:

Deploy Prometheus monitoring in Linux system, and configure alarm rules for running

applications and middleware.

Information:

MySQL default password qwe123456

Requirements:

1. Deploy monitoring services

Use the installation packages alertmanager-0.24.0.linux-amd64.tar.gz, node_exporter-1.3.1.linux-amd64.tar.gz, prometheus-2.36.2.linux-amd64.tar.gz under /data/package/ to set up promethues monitoring service

The installation directory of Prometheus is: /data/service/prometheus

The installation directory of alertmanager is: /data/service/alertmanager

The installation directory of node_exporter is: /data/service/node_exporter

The installation directory of mysqld_exporter is: /data/service/mysqld_exporter

The installation directory of redis_exporter is: /data/service/redis_exporter

The installation directory of nginx-vts-exporter is: /data/service/nginx-vts-exporter

2. Configure alarm rules

(1) Alarm when CPU utilization reaches 80%;

(2) Alarm when memory utilization reaches 80%;

(3) Alarm when disk utilization reaches 80%;

(4) Node status;

(5) MySQL survival status;

(6) Redis survival status;

(7) Nginx survival status;

(8) Java application survival state.

Module D network security management

Score: 100 points

Competition time: 180 minutes

Project background：

Engineers, the network management work of the company headquarters, Shanghai branch

and Wuhan Office has entered normal operation.

In order to ensure the network security of the company's network links and equipment, and the information security of various application systems, it is necessary to formulate the network security implementation plan and carry out drills in accordance with the relevant national standards, do a good job in the daily monitoring, early warning and disposal of network security, reasonably reinforce according to the importance of the problems, and improve the response ability to network security emergencies.

Please complete specific tasks within the specified time according to the information and data provided below.

Task 1: deploy and configure security devices

Task description:

Ensure the host security, including account security, IP protocol security and IPTABLE configuration. At the same time, according to the system deployment and configuration of the corresponding protection strategy, ensure the security of network configuration.

Requirements:

Task 1.1 Host security reinforcement

（1）Set the password policy. The minimum password length shall not be less than 16 characters, and the parameters and parameter values that must be used for this operation shall be submitted as Flag values;

（2）Setting password policy must meet the special characters of upper and lower case letters and numbers at the same time;

（3）Password policy: set the period of regular password modification to 30 days, and submit the parameters and parameter values that must be used in the operation command as Flag values;

（4）Login policy: only 3 login failures are allowed within one minute. If there are more than 3 login failures, the login account will be locked for 1 minute, and the parameters and parameter values that must be used by the operation command will be submitted as Flag values;

（5）Set the number of bash historical commands to 5, and submit the commands used in this operation as Flag values;

（6）IPTABLES sets the Linux system to prohibit others from Ping pass, and submits the command as a flag value;

（7）IPTABLES Linux setting disables port 23 and submits the command as a flag value;

（8）Set the firewall to allow the local machine to forward all data packets except ICMP Protocol, and submit the command as a flag value.

Task 1.2 Configure network security protections

（1）The firewall is located at the enterprise Internet exit. Please specify rules on the firewall to allow PCs in the intranet 10.1.1.0/24 network segment to access the Internet, and prohibit Internet users from accessing the intranet host with IP address 192.168.1.2;

（2）There is a server in the enterprise, which allows the office area with IP network segment 10.2.1.0/24 to access this server, and the security policy1 is configured. After running for a period of time, it is required to prohibit two temporary office PCs (10.2.1.1, 10.2.1.2) from accessing the server;

（3）It is often necessary to remotely manage the intranet devices in a system, and these intranet devices cannot be directly logged in remotely. Please use the SSL VPN function of the firewall to complete the configuration;

（4）Since the company cannot access the public network, please configure the NAT policy for the firewall to enable intranet users to access the Internet.

Task 2: detect network security vulnerabilities

Task description:

Detect network security vulnerabilities, including host scanning and information collection, data analysis, digital forensics, web security applications, and penetration testing.

Requirements:

Task 2.1 Host scanning and information collection

Service IP:172.17.224.2

（1）Use Nmap tool to scan the target drone service for TCP synchronous full connection, and submit the server information in the second line from bottom to top in the operation display result as flag values;

（2）Use Nmap tool to scan the target drone service with firewall to prohibit Ping, and submit

the parameters that must be used in the command used in this operation as flag values;

（3）Use Nmap tool to scan the target drone service with firewall to prohibit Ping, and submit the database service information in the operation display result as flag values;

（4）Use the Nmap tool to detect the service version information of the target drone for scanning, and submit the version information of the service in the third line from bottom to top in the operation display result as flag values;

（5）Use Nmap tool to conduct UDP scanning penetration test on the target drone, only scan port 53 and 111, and submit the status information of port 111 in the operation display result as flag values;

（6）Use Nmap tool to conduct RPC scanning penetration test on the target drone, and submit the parameters that must be used in the operation command as flag values;

（7）Use Nmap tool to conduct RPC scanning penetration test on the target drone, and submit the service information in the third line from bottom to top in the operation display result as flag values;

（8）Use Nmap tool to scan the service and version of the target drone, and submit the service status information corresponding to port 445 in the operation display result as flag values;

（9）Use the tool Nmap to perform system service and version scanning penetration test on the target drone, output information to the specified file test.xml in XML format, and submit the parameters that must be used to output information to the specified file in XML format as flag values;

（10）In the penetration test platform, use the command to initialize the MSF database and submit this command as flag values;

（11）In the penetration test platform, open MSF and use db_import to import the scanning results into the database and view the imported data. The command to view the data is submitted as flag values.

Task 2.2 Data analysis and digital forensics

Packet address:/headless/Desktop/hack.pcapng

（1）Use Wireshark to view and analyze the data package file hack.pcapng, and find the sqlpayload statement maliciously constructed by the user for the first time by analyzing the data package hack.pcapng, which proves the existence of SQL injection. Submit the payload statement of the malicious user as the flag value;

（2）Use Wireshark to view and analyze the data package file hack.pcapn, and submit the complete name of the data table in the payload statement as the flag value by analyzing the SQL statement of the data package hack.pcapn exploding the data name in the hacker;

（3）Use Wireshark to view and analyze the data package file hack.pcapn, and submit the hexadecimal value of the data table in the payload statement as the flag value by analyzing the SQL statement of the data package hack.pcapn exploding the data table in the hacker;

（4）Wireshark is used to view and analyze the data package file hack.pcapn. By analyzing the SQL statement of the data package hack.pcapn exploding the data table structure in the hacker, the hexadecimal values related to the data table and column in the payload statement are submitted as flag values;

（5）Use Wireshark to view and analyze the data package hack.pcapn, and submit the user name and password of the account as flag values by analyzing the account content of the system obtained by the hacker in the data package hack.pcapn;

（6）Use Wireshark to view and analyze the data package hack.pcapn, and submit the contents of the Trojan file as flag values by analyzing the Trojan file uploaded by the hacker in the system;

（7）Use Wireshark to view and analyze the data package hack.pcapn, and submit all the contents of root as flag values by analyzing the contents of the data package hack.pcapn executed by the hacker through Trojan files.

Task 2.3 Web security penetration test:

Server scenario user name and password: unknown

HTTP service address: http://172.17.224.2:8080/JSPClassNewsSystem

(1) Access the HTTP service address, construct the SQL injection point, construct the command execution, obtain the database name used by the system, and submit the database name as the flag value; for example [database name];

(2) Access the HTTP service address, construct the SQL injection point, construct the command execution, obtain and count the number of tables used in the database, and submit the counted number of tables as the flag value; for example [6];

(3) Access the HTTP service address, construct the SQL injection point, construct the command execution, obtain and count the tables in the database, and submit the table name as the flag value; For example [table 1; table 2];

(4) Access the HTTP service address, construct the SQL injection point, construct the command execution, obtain and count the fields in the user table, and submit the field name as the flag value; For example [field 1; field 2; field 3];
(5) Access the HTTP service of the target drone through the penetration machine, construct the SQL injection point, construct the command execution, obtain the password of the admin user, and submit the password as the flag value. For example [password];
(6) Access the HTTP service of the target drone through the penetration machine, construct the SQL injection point, construct the command execution, obtain the password of the user zledu, and submit the password as the flag value. For example [password].

Task 3: deploy cloud network security protection

Task description:

Complete the defense strategy of enterprise cloud resources and common attacks, complete SQL injection, XSS cross site, webshell upload, command injection, backdoor isolation, etc.

Requirements:
1. The client website www.test.com is injected with vulnerabilities and tampered in the page. Please use the cloud web application firewall, combined with the configuration of DNS resolution, to help the website shield web page vulnerabilities and tampering attacks, so as to avoid economic losses;
2. Port 80 of the server is used to provide web services. If the server deploys a website and does not open port 80, the website will definitely not be accessible. Please configure rules to make port 80 open;
3. Some hackers carry out DDoS attacks on business system www.test.com, resulting in frequent server paralysis, business failure, and huge losses. Please access DDoS to reduce network risk and reduce enterprise losses;
4. The customer's website needs to be upgraded. In consideration of data security, please make a full copy through the cloud database, and configure to keep the data backup for 30 days, with a backup cycle of 1 week.